030319 Instant Messaging Communications

Purpose: To identify the risks of using instant messaging and establish standards for mitigation of those risks.

STANDARD

If an agency or organization determines that the use of instant messaging (IM)[1] is critical to its mission, the agency head or his / her designee must document, in a risk assessment, the reasons for using the software and its compliance features including:

- A detailed business case.
- The circumstances under which IM can be used.
- The access controls that will ensure that the agency has taken sufficient steps to mitigate or isolate the associated threats.
- Any legal and regulatory requirements associated with information that may be used in electronic communications, such as requirements for confidentiality, security and record retention.[2]
- Architectural details.
- The capturing and logging the use of IM.

The risk assessment results shall be used to identify the policies and controls that are required to appropriately protect these communications.

Agencies must not use IM unless the risks have been identified and appropriate risk mitigation measures have been implemented or an approved deviation has been obtained from the State CIO. Agency users must install IM software as directed by their security or IT department. Agency users must not use, download, or install any nonstandard software without obtaining permission as defined by agency policy. Records and supporting documentation must be maintained by the agency so that compliance with this standard can be verified.

An agency's use of IM will be periodically assessed by the North Carolina Office of Information Technology Services for compliance with this standard.

GUIDELINES

The risk assessment for IM should include the following considerations:

- Communications sensitivity –
  - o What are the consequences of unauthorized or accidental access, modification, or loss of the communications?
  - o Is there a consequence for misdirected or incorrectly addressed messages?

[1] Instant Messaging (IM) covers a broad range of technologies that allow individuals to digitally communicate in real time over a LAN or the Internet. These technologies can require the installation of client software or they can be web based. IM is similar to a telephone conversation but uses text-based, not voice, communication. IM conversations can occur PC-to-PC, phone-to-phone, PC-to-phone and phone-to-PC. Personal computing (PC) devices include, but are not limited to, desktops, PDAs, laptops and smart phones.

[2] *See,* **120201** Managing Media Storage and Record Retention

- Denial of service and impact on business practices
  - Are communications time sensitive?
  - Is reliability and availability of the communications service a factor?
- Legal considerations
  - Are there requirements for proof of origin, delivery, and/or acceptance?
  - Is non-repudiation a factor such that the sender cannot claim that they did not send or receive a message?
- Remote user access –
  - Are controls needed to allow secure remote access to e-mail accounts?
- File Transfers / File Attachments –
  - Will the agency forbid or restrict the transfer of files between users to prevent the possible dissemination of malware?[3]

In addition,

- Agencies should deploy an IM service that will allow agencies to enforce policies of data retention, confidentiality, acceptable use, etc. When choosing a product, agencies should give consideration to those products that interoperate with public services. This is especially important if the agency regularly deals with the public over IM.

- Agencies interacting with the public over IM should consider taking steps to protect confidential information. Installation of pattern matching filters or key word filters should be considered in order to flag (and possibly drop) patterns that represent potential policy violations such as drivers license numbers, social security numbers, credit card numbers, passwords etc. Alerts can be sent to the user (pop up policy reminders) , system administrators, security officers, privacy officers etc.

- AntiVirus / Malware products should be purchased and deployed in order to protect IM users and the network from this attack vector. Policies should also be updated to handle the practice of sending file attachments or URLs over the IM system, and restrict its use as much as possible.

- Agencies should consider installing URL filtering or a web proxy in order to reduce threat of Spam over IM (SPIM) or phishing attacks via IM.

- Agencies should update their Acceptable Use Policies to incorporate the acceptable use of IM.[4]

[3] *See,* Statewide Information Technology Standards **030501** - Transferring and Exchanging Data and, **100301** – Using the Internet in and Acceptable Way.

[4] *See,* The State Chief Information Officer's policies found at http://www.scio.state.nc.us/sitPolicies.asp as well as Security Information Technology Standard **10031 –** Using the Internet in an Acceptable Way.

- Agencies should provide end users with annual security awareness training in order to advise them of new or changed IM policies as well as to educate them on current IM threats

ISO 27002: 2007 References
10.8.4 Electronic messaging

100301 Using the Internet in an Acceptable Way

Purpose: To establish a standard pertaining to the use of the State Network and the global Internet by state employees and other state network users.

STANDARD

While performing work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, state employees and other state network users shall be expected to use the State Network and the Internet responsibly and professionally and shall make no intentional use of these services in an illegal, malicious or obscene manner.

Each agency shall determine the extent of personal use its employees and other State Network users, under its control, may make of the State Network and the Internet.

Agencies that use the State Network shall prohibit users from the download and installation of unapproved software as defined by each agency's IT policies.

All files downloaded from a source external to the State Network shall be scanned for viruses, Trojan horses, worms or other destructive code for such harmful contents. This includes files obtained as email attachments and through any other file transfer mechanism. It shall be the responsibility of public employees and State Network users to help prevent the introduction or propagation of computer viruses. All agencies shall ensure that they have current software on their networks to prevent the introduction or propagation of computer viruses.

State employees and other state network users shall not access or attempt to gain access to any computer account which they are not authorized to access. They shall not access or attempt to access any portions of the State Network to which they are not authorized to have access. Public employees and other State Network users also shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to have access.

Operators of email services must create an abuse@<*host domain name*> account and other additional internal procedures to manage their email complaints. Users who receive email that they consider to be unacceptable according to this standard can choose to forward the original email message (including all headers) to the appropriate email abuse@<*host domain name*> account.

GUIDELINES

Agencies may want to address other acceptable use issues in their own internal policies on subjects such as use of instant messaging, and personal use of state computers.

ISO 27002 References

8.2.3	Disciplinary process
15.1.5	Prevention of misuse of information processing facilities